PATENTTI- JA REKISTERIHALLITUS
NATIONAL BOARD OF PATENTS AND REGISTRATION

Helsinki 9.7.2003

E T U O I K E U S T O D I S T U S
P R I O R I T Y D O C U M E N T

Hakija Applicant	**Nokia Corporation** **Helsinki**
Patenttihakemus nro Patent application no	**20021638**
Tekemispäivä Filing date	**12.09.2002**
Kansainvälinen luokka International class	**H04L**
Keksinnön nimitys Title of invention	

"Yhteysvastuun vaihtaminen"

Täten todistetaan, että oheiset asiakirjat ovat tarkkoja jäljennöksiä Patentti- ja rekisterihallitukselle alkuaan annetuista selityksestä, patenttivaatimuksista, tiivistelmästä ja piirustuksista.

This is to certify that the annexed documents are true copies of the description, claims, abstract and drawings originally filed with the Finnish Patent Office.

Pirjo Kaila
Tutkimussihteeri

Maksu 50 €
Fee 50 EUR

Maksu perustuu kauppa- ja teollisuusministeriön antamaan asetukseen 1027/2001 Patentti- ja rekisterihallituksen maksullisista suoritteista muutoksineen.

The fee is based on the Decree with amendments of the Ministry of Trade and Industry No. 1027/2001 concerning the chargeable services of the National Board of Patents and Registration of Finland.

Osoite: Arkadiankatu 6 A, P.O.Box 1160, FIN-00101 Helsinki, FINLAND
Puhelin: 09 6939 500
Telephone: + 358 9 6939 500
Telefax: 09 6939 5328
Telefax: + 358 9 6939 5328

Yhteysvastuun vaihtaminen

Keksinnön tausta

Keksintö liittyy yhteysvastuun vaihtamiseen ja erityisesti yhteysvastuun vaihtamiseen ja tunnelin päivittämiseen liityntälaitteiden välillä.

Peittoalueeltaan erittäin kattavia ja käyttäjän liikkuvuutta hyvin tukevia julkisia matkaviestinverkkoja varten kehitetyt datapalvelut ovat kehittyneet huomattavasti viime vuosina. Pakettivälitteinen GPRS-palvelu (General Packet Radio Service) tarjoaa GSM-verkkoja varten tehokkaan datavälityksen, jossa radiokapasiteettia on varattuna ainoastaan pakettien siirron aikana. 3GPP:n (Third Generation Partnership Project) standardoima kolmannen sukupolven UMTS-järjestelmä (Universal Mobile Telecommunications System) tulee tarjoamaan GSM/GPRS-verkkojakin suuremman datan välityskapasiteetin.

PLMN-verkkojen tarjoamien datapalveluiden lisäksi on kehitetty useita erilaisia langattomia paikallisia verkkoja, jotka tarjoavat hyvin rajallisella peittoalueelta laajakaistaisen langattoman datasiirtopalvelun. Eräitä tällaisia tekniikoita ovat IEEE 802.11 –pohjaiset WLAN-verkot. Näitä paikallisia verkkoja voidaan käyttää tarjoamaan erilaisissa aktiivikohdissa (hot spot), kuten toimistoissa tai lentokentillä, erittäin nopean datansiirron ja pääsyn Internetiin. Myös langattomien lähiverkkojen ja PLMN-verkkojen konvergoitumista on tapahtunut. Esimerkiksi GSM-teknologiaan perustuvia tukiasemia voidaan käyttää toimiston tietojärjestelmässä langattoman yhteyden järjestämiseen toimiston lähiverkkoon. Toisaalta myös langattomia lähiverkkoja varten on suunniteltu verkkoelementtejä, joiden avulla paikallinen verkko voi hyödyntää PLMN-verkkoa. Esimerkiksi IEEE 802.11-standardin mukaisia WLAN-verkkoja ja GSM-verkkoja varten on kehitetty verkkoelementtejä, joiden avulla WLAN-verkon kautta päästään GSM-verkon tarjoamiin todentamis- ja laskutuspalveluihin. PLMN-verkkojen ja langattomien lähiverkkojen yhteistoimintaa on suunniteltu myös pidemmälle niin, että langattomien lähiverkkojen tarjoaman radiorajapinnan kautta voitaisiin käyttää PLMN-verkkojen palveluita. UMTS-järjestelmässä, jota kutsutaan myös 3GPP-järjestelmäksi (3GPP System), langaton lähiverkko voisi toimia yhtenä liityntäalijärjestelmänä.

Viitaten kuvioon 1, paikallisesta verkosta voidaan järjestää päätelaitteelle TE tiedonsiirto IP-verkon yli vastinsolmuun CH (Corresponding Host) käyttämällä tunnelointia. Tällöin paikallisen verkon liityntälaitteen AD, esimerkiksi liityntäpisteen tai yhdyskäytävälaitteen, ja IP-verkon vastisolmun CH, esimerkiksi yrityksen intranet-verkon reunareitittimen, välille muodostetaan

tunneli. Tunneli on päästä-päähän polku, jossa siirrettävät datayksiköt siirretään läpinäkyvästi tunnelin päätepisteiden AP, CH välillä kapseloimalla datayksiköt MAC-kerroksen kehykseen. IP-verkoissa voidaan käyttää monia erilaisia tunnelointitekniikoita, joista yhtenä esimerkkinä on L2TP (Layer 2 Tunneling Protocol), jolla voidaan muodostaa virtuaalisia yksityisverkkoja (VPN; Virtual Private Network). Eräs toinen esimerkki tunnelointitekniikoista on Generic Routing Encapsulation (GRE), jota käytetään yleisesti IP-reitittimien välisissä tunneleissa.

Tunneleiden käyttö kuitenkin vaikeuttaa päätelaitteiden liikkuvuutta. Kun päätelaite siirtyy ensimmäisen liityntäpisteen peittoalueelta toisen liityntäpisteen peittoalueelle, sille ensimmäisen liityntäpisteen kautta järjestetty polku tulee vaihtaa toisen liityntäpisteen kautta kulkevaksi, eli on suoritettava yhteysvastuun vaihto (handover) toiseen liityntäpisteeseen. Jos tunnelin päätepisteenä on ensimmäinen liityntäpiste, myös tunnelin päätepiste on vaihdettava ensimmäisestä liityntäpisteestä toiseen päätepisteeseen. Tämä vaatisi, että tunnelin vastinesolmua päivitetään, eli siihen vaihdetaan tunnelin päätepisteeksi toinen liityntäpiste. Tunnetut tunnelointiratkaisut eivät kuitenkaan tue tunnelin päätepisteen vaihtamista. Ongelmaa on pyritty ratkaisemaan ylemmän tason neuvottelumekanismeilla. Esimerkiksi IP-liikkuvuusprotokollaa (Mobile IP) varten on määritetty signalointimekanismit, joiden mukaisesti kotiverkkoon saadaan päivitettyä päätelaitteen sijainti. Julkaisussa WO 0 235 738 on esitetty yhteysvastuun vaihtomenetelmä IP-liikkuvuusprotokollaa hyödyntävässä järjestelmässä. Menetelmässä päätelaitetta palvelevan etäagentin ja reitittimen välillä on tunneli. Kun päätelaitteelle suoritetaan yhteysvastuun vaihto toisen etäagentin alueelle, toinen etäagentti voi rekisteröityä kotiagenttiin, josta lähetetään sidonnan päivityspyyntö reitittimelle. Reititin voi päivittää tunnelin päätepisteeksi toisen etäagentin. Julkaisun WO 0 235 738 ratkaisussa on kuitenkin epäkohtia. Se soveltuu ainoastaan IP-liikkuvuusprotokollaa käyttävään järjestelmään. Päätepisteen vaihtaminen vaatii tätä tarkoitusta varten tarvittavalle signalointimekanismille tukea reitittimeltä, jota ei useinkaan löydy ainakaan vanhemmista reitittimistä. Päätepisteen vaihtaminen yleisesti tunnelin vastinsolmussa aiheuttaa lisäsignalointia järjestelmään ja viivekriittisille sovelluksille haitallista viivettä tiedonsiirtoon.

Keksinnön lyhyt selostus

Keksinnön tavoitteena on siten kehittää menetelmä ja menetelmän toteuttava laitteisto siten, että tunnelin vaihtamiseen vastinsolmussa liittyvät ongelmat voidaan välttää. Keksinnön tavoite saavutetaan menetelmällä, järjestelmällä ja liityntälaitteilla, joille on tunnusomaista se, mitä sanotaan itsenäisissä patenttivaatimuksissa. Keksinnön eräät edulliset suoritusmuodot ovat epäitsenäisten patenttivaatimusten kohteena.

Keksintö perustuu siihen täysin aiemmista ratkaisuista poikkeavaan oivallukseen, että käytetään tunnelointi-IP-osoitteena erityisesti päätelaitetta varten allokoitua osoitetta, joka säilyy, kun yhteysvastuu vaihdetaan ensimmäisestä liityntälaitteesta toiseen liityntälaitteeseen. Ensimmäisessä liityntälaitteessa on allokoitu tunnelointi-IP-osoite päätelaitteen tiedonsiirrolle vastinsolmuun muodostettavaa tunnelia varten, johon tunnelointi-IP-osoitteeseen tunneli on sidottu. Ensimmäisestä liityntälaitteesta siirretään ainakin allokoitu tunnelointi-IP-osoite toiseen liityntälaitteeseen vasteena sille, että on havaittu tarve vaihtaa päätelaitteen langaton yhteys toisen liityntälaitteen toteutettavaksi. Toisessa liityntälaitteessa määritetään sidonta tunnelointi-IP-osoitteen ja toisen liityntälaitteen verkkoliitynnän välille, eli näin ollen sidotaan tunneli toiseen liityntälaitteeseen. Tieto uudesta sidonnasta toisen liityntälaitteen verkkoliitynnän ja allokoidun tunnelointi-IP-osoitteen välillä lähetetään ainakin yhdelle järjestelmän käsittämälle verkkosolmulle.

Yhteysvastuun vaihtaminen (handover) on tulkittava laajasti tarkoittamaan mitä tahansa mekanismia, jolla tiedonsiirron mahdollistava looginen yhteys tai konteksti vaihdetaan toisen liityntälaitteen hoidettavaksi. Näin ollen myös pakettivälitteisen tiedonsiirtokontekstin vaihtaminen toisen liityntälaitteen hoitamaksi on yhteysvastuun vaihtamisen suorittamista, vaikka käyttäjädataa ei sillä hetkellä siirrettäisikään (piirikytkentäisissä verkoissa yhteysvastuun vaihtamisella tarkoitetaan tyypillisesti vain aktiivisena olevan puhelun siirtämistä). Toisen liityntäpisteen verkkoliitynnällä tarkoitetaan yleisesti mitä tahansa liityntää, johon tunneli toisesta liityntäpisteestä vastinsolmuun voidaan sitoa. Verkkoliityntä voi olla esimerkiksi Ethernet-liityntä.

Keksinnön mukaisen ratkaisun etuna on, että vastinsolmua ei tarvitse päivittää tunnelin toisen päätepisteen vaihtumisen takia. Tällöin voidaan toteuttaa aktiivisen yhteyden vaihtaminen liityntälaitteesta, esimerkiksi langattoman lähiverkon liityntäpisteestä toiseen, myös tunneloituja yhteyksiä käytettäessä. Ylempien kerrosten signalointiratkaisuja ei tarvita liikkuvuuden tukemi-

seksi, ja voidaan välttää kokonaan vastinsolmun päivittämiseen liittyvät ongelmat. Tunnelointiprotokolliin, tunnelien vastinsolmujen toteutuksiin, päätelaitteisiin tai päätelaitteen ja liityntälaitteiden välisiin standardeihin ei tarvita muutoksia. Koska tunnelin päätepistettä voidaan vaihtaa paikallisesti, voidaan välttää vastinsolmulle lähetettävien ja siltä vastaanotettavien signalointiviestien aiheuttama viive, mikä voi olla viivekriittisille sovelluksille tärkeää.

Keksinnön erään edullisen suoritusmuodon mukaisesti mainittu sidonta on sidonta verkkoliitynnän MAC-osoitteen ja tunnelointi-IP-osoitteen välillä. Tällöin aliverkon sisällä voidaan päivittää tarvittaessa aliverkon muihinkin verkkosolmuihin tieto uudesta sidonnasta, jonka jälkeen aliverkossa paketit välittyvät toiselle liityntälaitteelle siirtoyhteyskerroksen mekanismeja käyttäen.

Kuvioiden lyhyt selostus

Keksintöä selostetaan nyt lähemmin edullisten suoritusmuotojen yhteydessä, viitaten oheisiin piirroksiin, joista:

Kuvio 1 havainnollistaa tunnelointia;

Kuvio 2 havainnollistaa erästä paikallista verkkoa, jossa liityntäpisteestä voidaan järjestää tunneli useisiin erilaisiin vastinsolmuihin;

Kuvio 3 esittää keksinnön erään edullisen suoritusmuodon mukaista menetelmää;

Kuvio 4 esittää keksinnön erään edullisen suoritusmuodon mukaista menetelmää; ja

Kuvio 5 esittää signalointikaaviona yhteysvastuun vaihtoa keksinnön erään edullisen suoritusmuodon mukaisesti.

Keksinnön yksityiskohtainen selostus

Kuviossa 2 on havainnollistettu paikallista verkkoa BAN, josta liityntäpisteestä AP voidaan järjestää tunneli useisiin erilaisiin vastinsolmuihin CH. Paikallinen verkko BAN on erään edullisen suoritusmuodon mukaisesti jonkin IEEE 802.1x-standardin mukaista käyttäjän todentamista ja verkkoonpääsynvalvontaa käyttävä langaton lähiverkko, kuten IEEE 802.11i-standardin mukainen langaton lähiverkko. Keksintöä voidaan kuitenkin soveltaa myös muissa IEEE 802-pohjaisissa langattomissa lähiverkoissa tai muuntyyppisissä paikallisissa, tyypillisesti lisensioimattomalla taajuuskaistalla toimivissa verkoissa BAN, esimerkiksi BRAN-standardin (Broadband Radio Access Network) mukaisessa verkossa HomeRF-verkossa tai Bluetooth-verkossa. BRAN-standar-

dit käsittävät tyyppien 1 ja 2 HIPERLAN-standardit (High Performance Radio Local Area Network), HIPERACCESS- ja HIPERLINK-standardit.

Liityntäpiste AP hallitsee radiorajapintaa käytettävän radioteknologian mukaisesti, erään edullisen suoritusmuodon mukaisesti IEEE 802.11-standardin mukaisesti. IEEE 802.11 -spesifikaatiot määrittävät sekä fyysisen kerroksen että MAC-kerroksen protokollat tiedonsiirrolle radiorajapinnan yli. Tiedonsiirrossa voidaan käyttää infrapunaa tai kahta hajaspektritekniikkaa (Direct Sequence Spread Spectrum DSSS, Frequency Hopped Spread Spectrum FHSS). Molemmissa hajaspektritekniikoissa käytetään 2,4 gigahertsin kaistaa. MAC-kerroksella käytetään ns. CSMA/CA-tekniikkaa (Carrier Sense Multiple Access with Collision Avoidance). AP huolehtii myös radiorajapinnan datavirtojen silloittamisesta (Bridging) tai reitittämisestä muihin verkkosolmuihin, kuten muihin liityntäpisteisiin ja reitittimiin R, ja muista verkkosolmuista. Tyypillisesti paikallinen verkko BAN käsittää yhden tai useamman aliverkkoja, joiden käsittämät liityntäpisteet on kytketty toisiinsa ja ne siirtävät tietoja muihin IP-pohjaisiin verkkoihin IPNW aliverkon reitittimen R kautta. Päätelaite TE voi olla esimerkiksi integroitu kommunikointilaite, sylimikro (laptop computer), yhdistettynä radiopääsyn tarjoavaan laitteistoon (esim. WLAN-kortti), tai PDA-laitteen ja matkapuhelimen yhdistelmä.

Liityntäpiste AP voi muodostaa tunnelin, tyypillisesti reitittimen R kautta, IP-verkon vastinsolmun CH kanssa. Kuten kuviossa 2 on havainnollistettu, voi olla monia erityyppisiä vastinsolmuja CH eri verkoissa, joiden kanssa liityntäpisteestä AP voi olla tarve muodostaa tunneli päätelaitteen TE datan siirtämiseksi.

Vastinsolmu CH voi olla esimerkiksi julkisen matkaviestinverkon PLMN operointisolmu SGSN (Serving GPRS Support Node) CH (SGSN) tai yhdyskäytävätukisolmu GGSN (Gateway GPRS Support Node) CH (GGSN), jolloin voidaan hyödyntää PLMN-verkkojen palveluita paikallisen verkon kautta. PLMN voi olla toisen sukupolven verkko, esimerkiksi GSM/GPRS-verkko, tai kolmannen sukupolven verkko, esimerkiksi 3GPP-organisaation (3rd Generation Partnership Project) määrittämä UMTS-verkko (Universal Mobile Telecommunications System), jota kutsutaan myös 3GPP-järjestelmän verkoksi.

SGSN voi palvella PLMN-verkkoon liittyneitä matkaviestimiä ja tarjota päätelaitteelle TE esimerkiksi pääsyn PLMN-verkon palveluihin paikallisen verkon BAN kautta. Tällöin muodostamalla tunneli vastinsolmuna toimivaan SGSN:ään, CH (SGSN), paikallisesta verkosta voidaan hyödyntää operoin-

tisolmun SGSN tarjoamia palveluita. Esimerkiksi päätelaitteen laskutustietoja voidaan siirtää operointisolmuun SGSN. Operointisolmuun SGSN muodostettua tunnelia voitaisiin myös käyttää päätelaitteen siirtyessä SGSN:n kuuluvien tukiasemien alueelta liityntäpisteen AP alueelle tarjoamaan tiedonsiirtoyhteys edelleen PLMN-verkon ja SGSN:n kautta. Tällöin päätelaitteelle TE tarjottavaa palvelua ei tarvitsisi muuttaa siirtymisen takia ja tiedonsiirto voisi kulkea edelleen mm. saman GGSN:n kautta. Tämänkaltainen tilanne voi olla esimerkiksi siirryttäessä yrityksen sisäiseen verkkoon GPRS-verkon alueelta.

Yhdyskäytävätukisolmu GGSN tarjoaa yhdyskäytävätoiminnan PLMN-verkosta ulkopuolisiin verkkoihin, kuten Internetiin tai yrityksen intranetiin. Päätelaitteella TE, joka voi olla kaksi- tai monitoimimatkaviestin, voi olla sopimus koti-PLMN-verkon operaattorin kanssa ja käyttäjä voi haluta käyttää kotiverkon yhdyskäytäväsolmua GGSN:ä tiedonsiirron järjestämiseen muihin verkkoihin myös käyttäessään paikallisen verkon BAN palveluita. Tällöin liityntäpisteestä AP muodostetaan tunneli vastinsolmuun CH (GGSN), joka järjestää pääsyn muihin verkkoihin. GGSN voi tällöin tarjota myös laskutuspalveluita. Tunneli voi olla operointisolmun SGSN ja yhdyskäytäväsolmun GGSN välillä käytettävän GTP-tunnelointiprotokollan (GPRS Tunneling Protocol) mukainen. Eräs keksinnön mahdollisista sovelluskohteista onkin GTP-tunnelin yhteysvastuun siirtäminen. Vaikka GTP-protokollassa onkin keinot päivittää muuttunut SGSN yhdyskäytäväsolmulle GGSN, tämä päivittäminen tapahtuu tyypillisesti harvoin, paljon harvemmin kuin liityntäpisteiden AP väliset siirtymät langattomissa paikallisissa verkoissa BAN. Jos langattomasta lähiverkosta halutaan tunneloida GGSN:lle, olisi edullista, jos jokainen paikallinen verkko BAN näyttäisi vain yhdeltä loogiselta SGSN:ltä, jolloin paikallisen verkon BAN sisäinen liikkuvuus ei näkyisi GGSN:lle. Tämä mahdollistuu käyttämällä erään edullisen suoritusmuodon mukaista paikallista tunnelin siirtoa käyttäen siirryttäessä liityntäpisteestä AP toiseen. Vain paikallisten verkkojen BAN välisissä siirtymissä on tarpeen käyttää GTP-signalointia päätepisteen päivittämiseksi.

Erään edullisen suoritusmuodon mukaisesti PLMN-verkko käsittää tunnettujen verkkoelementtien lisäksi Iu-rajapintaa tukevan palvelusolmun BSN (Broadband Service Node) yhtä tai useampaa paikallista verkkoa BAN varten. Tässä suoritusmuodossa PLMN-verkon käyttäjä- ja signalointidata välitetään läpinäkyvästi langattoman liityntäpisteen AP ja IP-verkon yli. Onnistuneen todentamisen jälkeen (jonka joko BSN tai erillinen todentamispalvelin AS suorittaa) MS voi käyttää myös vierailtavan PLMN-verkon palveluita paikallisen ver-

kon BAN ja palvelusolmun BSN kautta. Palvelusolmun BSN toiminta vastaa monelta osin palvelevan radioverkko-ohjaimen RNC toimintaa. Palvelusolmun BSN toimintoja voivat olla:

- PLMN-verkon radiopääsyverkkoa, kuten UTRAN-verkkoa, varten määritettyjen RRC-signalointiprotokollien (Radio Resource Control) suorittaminen mahdollisesti BAN-spesifisten rajoitusten mukaisesti
- Korkeampien kerrosten PLMN-verkon, esimerkiksi UMTS-datavirtojen, kuten loogisten kanavien tai kuljetuskanavien, multipleksointi IP-pohjaisiin siirtopolkuihin paikalliseen verkkoon BAN ja demultipleksointi paikallisesta verkosta BAN
- Radioyhteyksien hallinta
- PLMN-verkon salauksen järjestäminen
- PLMN-verkon IP-otsikkokenttien kompressointi
- PLMN-verkon RLC-kerroksen (Radio Link Control) uudelleenlähetykset

Palvelusolmun BSN toiminnot voivat mahdollisesti myös sisältää paikallisen verkon BAN resurssien käytön seuraamisen BAN-operaattorin laskutuksen tarkistamiseksi. Paikallinen verkko BAN voi olla usean PLMN-verkon hyödyntämä. Paikallinen verkko BAN voi olla kytkettynä useaan palvelusolmuun BSN ja BSN voi olla kytketty yhteen tai useampaan paikalliseen verkkoon BAN. BSN voidaan jakaa erillisiin käyttäjätason (User Plane) yhdyskäytävä- ja ohjaustason (Control Plane) palvelintoimintoihin. BSN voi olla kytketty operointisolmuun SGSN, matkaviestinkeskukseen MSC (Mobile Switching Centre) ja mahdollisesti muihin PLMN-ydinverkon elementteihin standardien rajapintojen kautta. BSN voi olla myös kytketty muihin BSN-solmuihin tai PLMN-verkon radioaliverkkoon, esimerkiksi UTRAN-verkon RNC-elementteihin Iur-signalointirajapintojen kautta yhteysvastuun vaihtamisen tukemiseksi UTRAN-verkon sisällä tai UTRAN-verkkojen välillä. Tässä suoritusmuodossa MS sisältää välineet paikallisen verkon BAN alempien kerrosten (L1, L2) toteuttamiseksi ja välineet PLMN-verkon kanssa tiedonsiirtoon paikallisen verkon BAN kautta. Erään edullisen suoritusmuodon mukaisesti MS on kaksitoimipäätelaite (Dualmode Terminal), joka kykenee kytkeytymään paikallisen verkon BAN lisäksi myös PLMN-verkkoon, esimerkiksi UMTS-verkkoon UTRAN:n tukiasemien (Node B) kautta. Jotta matkaviestin MS kykenee muodostamaan yhtey-

den PLMN-verkkoon paikallisen verkon BAN kautta, on siinä oltava lisäksi seuraavat toiminnot:

- PLMN-verkon, esimerkiksi 3GPP-spesifikaatioiden määrittämien korkeampien kerrosten signalointiprotokollien toteuttaminen. Näitä protokollia ovat RRC (Radio Resource Control), istunnon hallinta (Session Management) ja liikkuvuuden hallinta (Mobility Management).

- PLMN-verkon käyttäjätason protokollien rajoitetun toiminnallisuuden suorittaminen ja käyttäjätason datan kommunikoiminen solmun BSN kanssa mahdolliset paikallisen verkon BAN aiheuttamat rajoitukset huomioiden. Näitä protokollia ovat RLC (Radio Link Control) ja PDCP (Packet Data Control Protocol).

- Korkeampien PLMN-verkon protokollakerrosten datavirtojen multipleksoiminen alempien kerrosten UDP/IP-pohjaisen tiedonsiirtoon ja käänteisesti vastaanotetun datan demultipleksoiminen päinvastoin PLMN-verkon datavirroiksi.

Tässä suoritusmuodossa liityntäpisteen AP ja palvelusolmun BSN (tunneloinnin kannalta siis CH(BSN)) välille voidaan muodostaa tunneli, jota käyttäen ylempien kerroksien PLMN-verkon signalointi– ja käyttäjädata voidaan siirtää paikallisen verkon BAN liityntäpisteen AP ja palvelusolmun BSN välillä.

Erään suoritusmuodon mukaisesti tunnelin vastinsolmuna toimii välityspalvelin CH(Proxy), joka yleisesti toimii välittimenä tiedonsiirrossa esimerkiksi Internetiin.

Erään suoritusmuodon mukaisesti tunnelin vastinsolmuna toimii reititin CH(R/FW) IP-verkon IPNW ja jonkin toisen verkon, esim. IP-pohjaisen intranetin rajalla. CH(R/FW) voi käsittää myös palomuuritoiminnallisuutta FW (Firewall). Tämä on eräs hyvin tyypillinen tunnelointiskenaario, jolloin esimerkiksi yrityksen sisäiseen verkkoon luodaan tunneli Internetin yli. Tällöin voidaan muodostaa VPN-yhteys paikallisessa verkossa BAN vierailevalle päätelaitteelle, VPN-toiminnallisuus usein asennetaan palomuuripalvelimeen. Siirrettävä data tyypillisesti salataan siirron ajaksi.

Edellisissä esimerkeissä voidaan käyttää mitä tahansa tunnelointiprotokollaa. Erään suoritusmuodon mukaisesti tunnelin vastinsolmuna toimii L2TP-protokollan mukainen L2TP Network Server (LNS), ja paikallisessa verkossa BAN tunnelin päätepisteessä on toteutettu L2TP-protokollan mukainen L2TP Access Concentrator (LAC). Erään toisen suoritusmuodon mukaisesti

tunnelointiprotokollana käytetään GRE-protokollaa, jolloin vastinsolmuna toimii reititin, joka tukee kyseistä tunnelointiprotokollaa.

On huomioitava, että liityntäpisteen AP sijaan tunnelin paikallisesta verkosta BAN voi myös muodostaa paikallisen verkon BAN pääsyohjain AC (Access Controller), jota voidaan myös kutsua PAC:ksi. Tämä pääsyohjain AC voi ohjata useaa liityntäpistettä, toimia yhdyskäytävänä ja sen toiminnallisuus voi sijaita esimerkiksi reititinlaitteessa R.

Kuviossa 3 on havainnollistettu keksinnön erään edullisen suoritusmuodon mukaista menetelmää. Vaiheessa 301 määritetään tunnelointiattribuutit ensimmäisen liityntälaitteen, esimerkiksi AP tai R, ja vastinsolmun CH välille. Tarvittavia tunnelointiattribuutteja, ainakin vastinsolmun CH IP-osoite, siirretään 302 ensimmäiselle liityntälaitteelle.

Tunnelointiattribuutit voidaan määrittää 301 ja siirtää 302 esimerkiksi ensimmäisen liityntälaitteen ja vastinsolmun CH välisessä signaloinnissa päätelaitteelta TE tai vastinsolmulta CH (tai sen kautta) tulleen palvelupyynnön perusteella. Erään suoritusmuodon mukaisesti tunnelointiattribuutit määritetään 301 osana päätelaitteen TE todentamista ennen tunnelin järjestämistä vastinsolmuun CH. Käytössä voi olla todentamispalvelin AS, erään suoritusmuodon mukaan RADIUS-palvelin, joka siirtää tunnelointiattribuutit paikallisen verkon ensimmäiselle liityntälaitteelle, jos todentaminen on onnistunut. Eräs esimerkki todentamisesta, jossa tunnelointiattribuutit voidaan määrittää ja siirtää langattoman lähiverkon liityntälaitteelle, on IEEE802.1x-todentamismekanismin soveltaminen RADIUS-palvelimen kanssa. Tällöin IEEE 802.1x-todentajana toimiva liityntäpiste AP pyytää päätelaitteen TE todentamista RADIUS-palvelinta, joka määrittää myös tunnelointiattribuutit, ja lähettää ne liityntäpisteelle AP, jos todentaminen on onnistunut. Tämänkaltaista todentamisprosessia on esitetty Internet-luonnoksessa "*IEEE 802.1x RADIUS Usage Guidelines*", Congdon et al., 17. kesäkuuta 2002, 29 sivua.

Ensimmäisessä liityntälaitteessa allokoidaan 303, erään edullisen suoritusmuodon mukaisesti vasteena onnistuneelle todentamiselle ja vastaanotetuille tunnelointiattribuuteille, päätelaitteelle TE sen tiedonsiirtoa varten IP-osoite ja päätelaitteen tiedonsiirrolle muodostettavaa tunnelia varten tunnelointi-IP-osoite, jota käytetään päätelaitteen dataa siirtävän tunnelin päätepisteenä. Tiedonsiirtoa varten käyttöön tuleva IP-osoite voidaan allokoida myös erillisessä DHCP-palvelimessa (Dynamic Host Configuration Protocol), vaihtoehtoisesti käytetään kiinteitä IP-osoitteita, jolloin kyseistä IP-osoitetta ei allokoida.

Ensimmäisessä liityntälaitteessa sidotaan 304 tunnelointiattribuuttien määrittämä tunneli tunnelointi-IP-osoitteeseen. Tällöin ensimmäisessä liityntälaitteessa on määritetty tunneli, jonka päätepisteinä ovat tunnelointi-IP-osoite ja vastinsolmun IP-osoite. Tämän jälkeen tiedonsiirto tunnelin kautta voi alkaa 305, jolloin liityntälaite kapseloi päätelaitteelta tulevat paketit vastinsolmulle CH ja vastaavasti purkaa kapseloinnin vastinsolmulta lähetetyistä ja päätelaitteelle kohdistetuista paketeista ja välittää datan päätelaitteelle TE langatonta linkkiä käyttäen. Tunnelin toisena päätepisteenä toimivaan tunnelointi-IP-osoitteeseen kohdistetut paketit siis välitetään ensimmäisen liityntälaitteen verkkoliityntään, edullisesti verkkoliitynnän MAC-osoitteeseen. Tunnelikohtaisten tunnelointi-IP-osoitteiden käyttäminen liityntälaitteessa poikkeaa olennaisesti tavanomaisista tunnelointiratkaisuista, joissa tunnelin päätepisteet käyttävät omia IP-osoitteitaan tunnelin päätepisteen tunnisteina.

Viitataan kuvioon 4, jossa on kuvattu seuraavia vaiheita erään edullisen suoritusmuodon mukaisessa menetelmässä. Kun on havaittu tarve 401 vaihtaa päätelaitteen langaton yhteys toisen liityntälaitteen toteutettavaksi, siirretään 402 ensimmäisestä liityntälaitteesta tunnelointiattribuutteja, erityisesti vastinsolmun IP-osoite ja päätelaitteelle ensimmäisessä liityntälaitteessa allokoitu tunnelointi-IP-osoite, sekä mahdollinen muu päätelaitteeseen liittyvä tilatieto toiseen liityntälaitteeseen.

Tarve yhteysvastuun vaihdolle 401 tyypillisesti aiheutuu päätelaitteen siirtyessä toisen liityntälaitteen peittoalueelle, jolloin toisen liityntälaitteen kautta voidaan saada päätelaitteelle TE laadultaan parempi radiolinkki. Erään suoritusmuodon mukaisesti, kun päätelaitteessa TE on määritetty tarve vaihtaa toiseen liityntälaitteeseen, se lähettää palvelupyynnön toiseen liityntälaitteeseen, jolloin päätelaitteelle TE muodostetaan tiedonsiirtoyhteys toiseen liityntälaitteeseen. Toinen liityntälaite havaitsee, että päätelaitteella TE on jo yhteys ensimmäisen liityntälaitteen kanssa. Tällöin esimerkiksi todentamista ei ole välttämätöntä uudestaan suorittaa, vaan toinen liityntälaite voi pyytää yhteyteen liittyviä tietoja ensimmäiseltä liityntälaitteelta esimerkiksi IAPP-protokollaa (Inter Access Point Protocol) käyttäen. Vasteena pyynnölle, ensimmäinen liityntälaite havaitsee tarpeen yhteysvastuun vaihdolle ja suorittaa vaiheen 402, ja tämän jälkeen se voi poistaa alkuperäisen sidonnan tunnelointi-IP-osoitteen ja verkkoliityntänsä välillä. IAPP-protokolla on valmistajakohtainen, joten yhteysvastuun vaihto liityntälaitteesta toiseen voidaan toteuttaa monella eri tapaa. Oleellista on, että kaikki päätelaitteeseen liittyvä tilatieto siirretään alkupe-

räisestä liityntälaitteesta toiseen liityntälaitteeseen. Esim. IEEE 802.11-protokollassa yhteysvastuun vaihdossa päätelaite kertoo ensimmäisen liityntälaitteen MAC-osoitteen toiselle liityntälaitteelle. Tällöin toinen liityntälaite lähettää viestin ensimmäiselle liityntälaitteelle. Vasteena tälle viestille ensimmäinen liityntälaite lähettää päätelaitteeseen liittyvän kontekstin toiselle liityntälaitteelle.

Toiselle liityntälaitteelle siirrettävät 402 tunnelointiattribuutit käsittävät ainakin osan seuraavista: päätelaitteen tunnelille paikallisesti allokoitu tunnelointi-IP-osoite, vastinsolmun IP-osoite, käytettävään tunnelointiprotokollaan liittyviä attribuutteja tai tilatietoja, kuten L2TP-yhteyden tilatietoja, erilaisia salaukseen ja yleisesti turvallisuuteen liittyviä attribuutteja, kuten IPsec-kontekstin attribuutteja. Erään edullisen suoritusmuodon mukaisesti käytetään IAPP-protokollaa kyseisten tietojen siirtämiseen toiselle liityntälaitteelle.

Toisessa liityntälaitteessa määritetään 403 sidonta tunnelointiattribuuttien määrittämän tunnelin ja toisen liityntälaitteen välille, erityisesti tunnelointi-IP-osoitteen ja toisen liityntälaitteen verkkoliitynnän, edullisesti verkkoliitynnän MAC-osoitteen, välille. Tällöin toinen liityntälaite konfiguroi tunnelin alkupisteen yhteen sen käsittämistä langallisen verkon rajapinnoista. Tieto uudesta sidonnasta toisen liityntälaitteen MAC-osoitteen ja mainitun tunnelointi-IP-osoitteen välillä lähetetään 404 ainakin yhdelle verkkosolmulle. Edullisesti tämä tieto lähetetään ainakin yhdelle paikallisen verkon BAN käsittämälle reitittimelle R. Tyypillisesti liityntälaitteet kuuluvat samaan aliverkkoon, jolloin riittää, että aliverkon reunalla (ulkopuoliseen IP-verkkoon IPNW nähden) sijaitsevan reitittimen sidostauluun päivitetään uusi merkintä tunnelointi-IP-osoitteen ja toisen liityntälaitteen MAC-osoitteen sidonnasta, joka korvaa ensimmäisen liityntälaitteen sidonnan tunnelointi-IP-osoitteen ja ensimmäisen liityntälaitteen MAC-osoitteen välillä. Tämä voidaan toteuttaa tavanomaisia linkkikerroksen mekanismeja käyttäen, eikä toiminnallisuus vaadi reitittimeltä mitään uusia ominaisuuksia. Luonnollisesti uusi sidonta tunnelointi-IP-osoitteen ja toisen liityntälaitteen MAC-osoitteen välillä voidaan välittää mille tahansa saman aliverkon solmulle. Päivityksen jälkeen tietoja päätelaitteelle/päätelaitteelta vastinsolmulta/vastinesolmulle siirretään 405 toiseen liityntälaitteeseen/toisesta liityntälaitteesta järjestettyä sidontaa käyttäen. Keksintö ei myöskään vaadi mitään muutoksia päätelaitteeseen TE; langattoman linkin siirtäminen ensimmäisestä liityntälaitteesta toiseen liityntälaitteeseen voidaan suorittaa jo tunnettuja mekanismeja käyttäen.

On huomioitava, että paikallisen verkon BAN konfiguraatio voi olla sellainen, ettei toisen liityntälaitteen ole tarpeen lähettää tietoa sidonnasta millekään muulle verkkosolmulle, vaan riittää, että se päivittää (404) sidonnan omaan muistiinsa. Tässä tapauksessa verkkosolmulla tarkoitetaan siis toista liityntälaitetta.

Edellä on havainnollistettu erilaisia tunnelointiskenaarioita. Keksintöä voidaan soveltaa mitä tahansa tunnelointiprotokollaa soveltavassa järjestelmässä. Eräitä tunnelointiprotokollia, joita voidaan käyttää, ovat jo mainittu L2TP, GRE, IP-in-IP Tunneling, , Point-to-Point Tunneling Protocol (PPTP), IP Encapsulating Security Payload in the Tunnel-mode (ESP), IP Authentication Header in the Tunnel-mode (AH), Ascend Tunnel Management Protocol (ATMP), Layer Two Forwarding (L2F), Bay Dial Virtual Services (DVS), ja Virtual Tunneling Protocol (VTP). Kuten edellä mainittiin, erään edullisen suoritusmuodon mukaisesti myös GTP-tunneli voidaan vaihtaa paikallisesti, jolloin GTP-tunneliin liittyvät tiedot siirretään ensimmäisestä liityntälaitteesta toiseen liityntälaitteeseen, joka ottaa ne käyttöön.

Kuviossa 5 on vielä havainnollistettu signalointikaaviona yhteysvastuun vaihtamiseen liittyviä viestejä keksinnön erään edullisen suoritusmuodon mukaisesti, jossa käytetään IAPP-protokollaa ja a) IPv4-protokollaa tai b) IPv6-protokollaa. Kun on tarve vaihtaa päätelaitteen TE yhteysvastuu ensimmäisestä liityntäpisteestä AP1 toiseen liityntäpisteeseen AP2, AP1 lähettää toiselle liityntäpisteelle AP2 tunnelointiattribuutteja ja tunnelointi-IP-osoite käyttäen tarkoituksenmukaista IAPP-viestiä [IAPP message] 501. AP2 muodostaa sidonnan 502 edellä havainnollistetulla tavalla tunnelointi-IP-osoitteen ja MAC-osoitteensa välille. AP2 lähettää 503 reitittimelle R a) IPv4-protokollaa käyttävässä järjestelmässä lähettämällä ARP-taulun (Address Resolution Protocol] päivitysviestin [Gratuitous ARP], minkä perusteella R päivittää ARP-tauluaan. Jos järjestelmässä on käytössä IPv6-protokolla, AP2 lähettää 503 b) IPv-6 protokollan mukaisen ilman pyyntöä lähetetyn mainosviestin [Unsolicited Neighbor Advertisement], jonka perusteella R päivittää naapuritaulukkoaan. Viestin 503 jälkeen reitittimen vastaanottamat paketit, joissa tunnelointi-IP-osoite on kohdeosoitteena, välitetään automaattisesti toiselle liityntäpisteelle AP2. Voi myös olla tilanteita, joissa verkon solmu tiedustelee vastaanottajaa (MAC-osoitetta) vastaanotetulle paketille, jossa tunnelointi-IP-osoite on kohdeosoitteena. Tällöin yhteysvastuun vaihdon jälkeen AP2 vastaa omalla MAC-osoitteellaan. Edellä esitetystä poiketen on myös mahdollista, että ensimmäinen liityntäpiste

AP1 päivittää (503 tai 504) ainakin yhden verkkosolmun sidontatietoja toisen liityntäpisteen AP2 sijaan.

Erään suoritusmuodon mukaisesti ensimmäinen liityntäpiste (AP1) voi välittää edelleen sille tulevia paketteja toiselle liityntäpisteelle (AP2). Tällöin ensimmäisen liityntäpisteen reititystauluun lisätään päätelaitteelle tilapäinen reitti toiseen liityntäpisteeseen, eli muutetaan alkuperäistä sidontaa ensimmäisessä liityntäpisteessä osoittamaan toisen liityntäpisteen MAC-osoitteeseen. Lisätty sidonta voidaan poistaa esimerkiksi ennalta määritetyn kynnysajan kuluttua. Tätä suoritusmuotoa käyttäen voidaan välttää tai ainakin vähentää vaihdon aikana lähetettyjen pakettien hukkaamista.

Keksinnön erään edullisen suoritusmuodon mukainen paikallinen tunnelin päivitys mahdollistaa vastinsolmuun päätepisteen vaihtumisesta johtuvasta signaloinnista aiheutuvan viiveen välttämisen, mitä havainnollistaa seuraava esimerkki: Oletetaan, että tunnelin vastinsolmu lähettää paketin päätelaitteelle TE. Sillä aikaa kun paketti on matkalla, liityntäpiste vaihtuu päätelaitteelle TE. Uusi liityntäpiste päivitetään (kuviossa 5 viestit 503, 504) paikallisesti linkkikerroksen paikallisen verkon BAN solmuihin esim. ARP-protokollalla. Tämän jälkeen tunneloitu paketti saapuu paikallisen verkon BAN solmun linkkikerrokselle. Se reitittyy aivan oikein uuteen päätepisteeseen (AP2), vaikka se lähetettiin ennen yhteysvastuun vaihtumista (ennen vaihetta 501).

Erään vaihtoehtoisen suoritusmuodon mukaisesti tunnelointi-IP-osoitteena käytetään samaa osoitetta kuin mitä päätelaite TE käyttää, eli osoitetta, joka tyypillisesti allokoidaan paikallisessa verkossa BAN, kun päätelaite on todennettu, ja lähetetään sitten päätelaitteelle. Tällöin liityntälaite (ensimmäinen tai toinen) käyttää siis tunnelin pääteosoitteena tunnelointi-IP-osoitetta, joka sattuu olemaan myös päätelaitteen TE tunniste. Tällöin liityntälaitteen MAC-osoitteeseen välitetään kyseiseen IP-osoitteeseen kohdistetut paketit, jotka vastaanotetaan paikallisessa verkossa BAN. Samaa IP-osoitetta käytetään siis kahdella tasolla, eli kapseloidun paketin lähde/kohdeosoitteena ja kapseloidun paketin sisältämän IP-paketin lähde/kohdeosoitteena. Liityntälaite on järjestetty välittämään tunnelista vastaanotetut paketit päätelaitteelle TE ja lähettämään päätelaitteesta TE vastaanotetut paketit tunneliin käyttäen kyseistä IP-osoitetta. Yhteysvastuun vaihtaminen ensimmäisestä liityntälaitteesta toiseen liityntälaitteeseen voidaan suorittaa edellä kuvioiden 4 ja 5 yhteydessä havainnollistetulla tavalla, jolloin tunnelointi-IP-osoitteeseen sidotaan toisen liittymälaitteen MAC-osoite. Jos paikallisessa verkossa lähetään päätelaitteelle

TE kohdistettuja paketteja esimerkiksi jostain muusta liityntäpisteestä (eli ilman tunnelia), paketit välitetään voimassa olevan sidoksen perusteella päätelaitetta palvelevalle liityntäpisteelle, joka muuttaa pakettien MAC-osoitteeksi päätelaitteen TE MAC-osoitteen ja edelleenlähettää ne päätelaitteelle TE. Vastaavasti kun palveleva liityntälaite vastaanottaa päätelaitteelta paketin, joka ei ole tarkoitettu tunnelin kuljetettavaksi, liityntälaite vain edelleenlähettää paketin kohdeosoitteen mukaisesti. Vaihtoehtoisesti tunnelointi-IP-osoite on sidottu päätelaitteen TE MAC-osoitteeseen, jolloin liityntäpisteiden siltausprotokollien ansiosta oikea liityntäpiste osaa välittää terminaalin paketit ilmatielle. Tällöin liityntäpiste tunneloi ja purkaa tunnelia osana siltausta.

Vielä erään suoritusmuodon mukaisesti paikallisen verkon BAN liityntäpiste AP (tai pääsyohjain AC) toimii IP-liikkuvuusprotokollan mukaisena liikkuvana solmuna (Mobile Node; MN). Tällöin liityntäpiste voidaan periaatteessa siirtää mihin tahansa verkkoon, myös aliverkkojen välillä, ja IP-liikkuvuusprotokolla pitää huolen siitä että vastinsolmun paketit löytävät aina perille. Edellä havainnollistettua tunnelin vaihtoa voidaan hyödyntää myös tässä suoritusmuodossa. Tällöin vaihdettaessa tunnelia uudelle liityntäpisteellä AP (tai pääsyohjaimelle AC) siirretään myös IP-liikkuvuusasiakaslaitteen tila, eli mahdolliset todentamisavaimet, kotiagentin osoite, ja tilatiedot sidonnoista (mobility bindings). Liityntäpisteen oma IP-osoite toimisi tällöin IP-liikkuvuusprotokollassa käytettävänä care-of –osoitteena, tunnelointi-IP-osoite (jota siis ei vaihdeta liityntäpistettä vaihdettaessa) toimisi IP-liikkuvuusprotokollan mukaisena kotiosoitteena, ja verkkosolmu, jolle tieto uudesta sidonnasta päivitetään, on kotiagentti (joka siis tyypillisesti sijaitsee paikallisen verkon BAN ulkopuolella). Eli kun tunnelia vaihdetaan toiseen liityntäpisteeseen, päivitetään tieto sidonnasta tunnelointi-IP-osoitteen ja toisen liityntäpisteen verkkoliitynnän IP-osoitteen välillä kotiagentille.

Liityntäpisteet AP käsittävät yhden tai useampia prosessoreita ja muistia, joita käyttäen keksinnölliset välineet, joiden eräitä suoritusmuotoja on havainnollistettu kuvioissa 2-5, voidaan toteuttaa. Tällöin keksinnölliset välineet toteutetaan prosessointiyksikössä suoritettavalla tietokoneohjelmakoodilla. On myös mahdollista käyttää kovo-ratkaisuja tai kovo- ja ohjelmistoratkaisuiden yhdistelmää toteuttamaan keksinnölliset välineet.

Alan ammattilaiselle on ilmeistä, että tekniikan kehittyessä keksinnön perusajatus voidaan toteuttaa monin eri tavoin. Keksintöä voidaan soveltaa myös muissa kuin paikallisen verkon käsittävissä tietoliikennejärjestelmis-

sä, esimerkiksi PLMN-verkon käsittämissä järjestelmissä, joissa käytetään tunnelointia. Keksintö ja sen suoritusmuodot eivät siten rajoitu yllä kuvattuihin esimerkkeihin vaan ne voivat vaihdella patenttivaatimusten puitteissa.

Patenttivaatimuks t

1. Menetelmä langattoman päätelaitteen yhteysvastuun vaihtamiseksi tietoliikennejärjestelmässä, jossa päätelaitteelle on järjestetty langaton yhteys ensimmäiseen liityntälaitteeseen, josta on edelleen järjestetty tunneli vastinsolmuun päätelaitteen tiedonsiirtoa varten,

t u n n e t t u siitä, että:

ensimmäisessä liityntälaitteessa on allokoitu tunnelointi-IP-osoite päätelaitteen tiedonsiirrolle muodostettavaa tunnelia varten, johon mainittuun tunnelointi-IP-osoitteeseen tunneli on sidottu, jossa menetelmässä:

siirretään ensimmäisestä liityntälaitteesta ainakin mainittu tunnelointi-IP-osoite toiseen liityntälaitteeseen vasteena sille, että on havaittu tarve vaihtaa päätelaitteen langaton yhteys toisen liityntälaitteen toteutettavaksi;

määritetään toisessa liityntälaitteessa sidonta mainitun tunnelointi-IP-osoitteen ja toisen liityntälaitteen verkkoliitynnän välille, ja

päivitetään tieto mainitusta uudesta sidonnasta toisen liityntälaitteen verkkoliitynnän ja mainitun tunnelointi-IP-osoitteen välillä ainakin yhdelle järjestelmän käsittämälle verkkosolmulle.

2. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että

määritetään todentamispalvelimessa tunnelointiattribuutteja, ainakin vastinsolmun IP-osoite ja päätelaitteelle ensimmäisessä liityntälaitteessa allokoitu mainittu tunnelointi-IP-osoite, osana päätelaitteen todentamista ennen tunnelin järjestämistä vastinsolmuun,

välitetään tunnelointiattribuutteja ensimmäiselle liityntälaitteelle vasteena onnistuneelle todentamiselle,

allokoidaan ensimmäisessä liityntälaitteessa päätelaitteelle päätelaitteen tiedonsiirrossa käyttämä IP-osoite ja päätelaitteen tiedonsiirrolle muodostettavaa tunnelia varten mainittu tunnelointi-IP-osoite, jota käytetään päätelaitteen dataa siirtävän tunnelin päätepisteenä,

sidotaan ensimmäisessä liityntälaitteessa tunnelointiattribuuttien määrittämän tunneli mainittuun tunnelointi-IP-osoitteeseen,

muodostetaan tunneli, jonka päätepisteinä ovat mainittu tunnelointi-IP-osoite ja vastinsolmun IP-osoite, minkä jälkeen tiedonsiirto mainittuun tunnelointi-IP-osoitteeseen välitetään mainitun ensimmäisen liityntälaitteen liityntärajapinnan verkkoliityntään.

3. Patenttivaatimuksen 1 tai 2 mukainen menetelmä, t u n n e t t u siitä, että

siirretään tietoja päätelaitteen ja vastinsolmun välillä päivittämisen jälkeen toiselle liityntälaitteelle järjestettyä sidontaa käyttäen.

4. Jonkin edellisen patenttivaatimuksen mukainen menetelmä, t u n n e t t u siitä, että mainittu verkkosolmu on reititin paikallisessa verkossa.

5. Jonkin edellisen patenttivaatimuksen mukainen menetelmä, t u n n e t t u siitä, että mainittu sidonta on sidonta verkkoliitynnän MAC-osoitteen ja mainitun tunnelointi-IP-osoitteen välillä.

6. Jonkin edellisen patenttivaatimuksen mukainen menetelmä, t u n n e t t u siitä, että järjestelmä tukee IPv6-protokollaa, jolloin tieto uudesta sidonnasta lähetetään ainakin yhdelle ensimmäiseen liityntälaitteeseen ja toiseen liityntälaitteeseen liitetylle verkkosolmulle sen reititystaulukkoon Neighbour Discovery-protokollaa käyttäen.

7. Jonkin patenttivaatimuksen 1-5 mukainen menetelmä, t u n n e t t u siitä, että järjestelmä tukee IPv4-protokollaa, jolloin tieto uudesta sidonnasta lähetetään ainakin yhdelle ensimmäiseen liityntälaitteeseen ja toiseen liityntälaitteeseen liitetylle verkkosolmulle sen ARP-taulukkoon (Address Resolution Protocol) ARP-protokollaa käyttäen.

8. Jonkin edellisen patenttivaatimuksen mukainen menetelmä, t u n n e t t u siitä, että ensimmäinen liityntälaite ja toinen liityntälaite ovat langattoman lähiverkon liityntäpisteitä, jotka on liitetty langallisen lähiverkon kautta toisiinsa.

9. Tietoliikennejärjestelmä, joka ainakin käsittää ensimmäisen liityntälaitteen, toisen liityntälaitteen ja päätelaitteen, missä

ensimmäinen liityntälaite on järjestetty tarjoamaan päätelaitteelle langattoman yhteyden ja muodostamaan tunnelin vastinsolmun ja ensimmäisen liityntälaitteen välille päätelaitteen tiedonsiirtoa varten,

t u n n e t t u siitä, että:

ensimmäinen liityntälaite on järjestetty allokoimaan tunnelointi-IP-osoitteen päätelaitteen tiedonsiirrolle muodostettavaa tunnelia varten, johon mainittuun tunnelointi-IP-osoitteeseen tunneli on sidottu,

ensimmäinen liityntälaite on järjestetty siirtämään ainakin mainitun tunnelointi-IP-osoitteen toiseen liityntälaitteeseen vasteena sille, että on havaittu tarve vaihtaa päätelaitteen langaton yhteys toisen liityntälaitteen toteutettavaksi;

toinen liityntälaite on järjestetty muodostamaan sidonnan mainitun tunnelointi-IP-osoitteen ja toisen liityntälaitteen verkkoliitynnän välille, ja

toinen liityntälaite on järjestetty päivittämään tiedon mainitusta uudesta sidonnasta toisen liityntälaitteen verkkoliitynnän ja mainitun tunnelointi-IP-osoitteen välillä ainakin yhdelle järjestelmän käsittämälle verkkosolmulle.

10. Patenttivaatimuksen 9 mukainen tietoliikennejärjestelmä, t u n n e t t u siitä, että tietojen siirtäminen päätelaitteen ja vastinsolmun välillä päivittämisen jälkeen on järjestetty tietoliikennejärjestelmässä toiselle liityntälaitteelle järjestettyä sidontaa käyttäen.

11. Patenttivaatimuksen 9 tai 10 mukainen tietoliikennejärjestelmä, t u n n e t t u siitä, että mainittu verkkosolmu on reititin paikallisessa verkossa.

12. Patenttivaatimuksen 9, 10 tai 11 mukainen tietoliikennejärjestelmä, t u n n e t t u siitä, että mainittu sidonta on sidonta verkkoliitynnän MAC-osoitteen ja tunnelointi-IP-osoitteen välillä.

13. Liityntälaite tietoliikenneverkkoa varten, joka liityntälaite on järjestetty tarjoamaan päätelaitteelle langattoman yhteyden ja muodostamaan tunnelin vastinsolmun ja liityntälaitteen välille päätelaitteen tiedonsiirtoa varten,

t u n n e t t u siitä, että:

liityntälaite on järjestetty allokoimaan tunnelointi-IP-osoitteen päätelaitteen tiedonsiirrolle muodostettavaa tunnelia varten, johon mainittuun tunnelointi-IP-osoitteeseen tunneli on sidottu, ja

liityntälaite on järjestetty lähettämään ainakin mainitun tunnelointi-IP-osoitteen toiseen liityntälaitteeseen vasteena sille, että on havaittu tarve vaihtaa päätelaitteen langaton yhteys toisen liityntälaitteen toteutettavaksi.

14. Patenttivaatimuksen 13 mukainen liityntälaite, t u n n e t t u siitä, että mainittu sidonta on sidonta verkkoliitynnän MAC-osoitteen ja tunnelointi-IP-osoitteen välillä.

15. Patenttivaatimuksen 13 tai 14 mukainen liityntälaite, t u n n e t t u siitä, että liityntälaite on järjestetty muuttamaan tunnelointi-IP-osoitteen sidonnan tilapäisesti osoittamaan toisen liityntälaitteen verkkoliityntään.

16. Liityntälaite tietoliikenneverkkoa varten, joka liityntälaite käsittää välineet langattoman yhteyden tarjoamiseksi päätelaitteelle ja välineet tunnelin muodostamiseksi vastinsolmun ja liityntälaitteen välille päätelaitteen tiedonsiirtoa varten, t u n n e t t u siitä, että:

liityntälaite on järjestetty vastaanottamaan ainakin päätelaitteen tiedonsiirrolle muodostettavaa tunnelia varten allokoidun tunnelointi-IP-osoitteen toiselta liityntälaitteelta vasteena sille, että on havaittu tarve vaihtaa päätelaitteen langaton yhteys liityntälaitteen toteutettavaksi.

liityntälaite on järjestetty muodostamaan sidonnan mainitun tunnelointi-IP-osoitteen ja verkkoliityntänsä välille, ja

liityntälaite on järjestetty päivittämään tiedon mainitusta uudesta sidonnasta verkkoliityntänsä ja mainitun tunnelointi-IP-osoitteen välillä ainakin yhdelle järjestelmän käsittämälle verkkosolmulle.

17. Patenttivaatimuksen 16 mukainen liityntälaite, t u n n e t t u siitä, että

liityntälaite on järjestetty päivityksen jälkeen siirtämään tietoja päätelaitteen ja vastinsolmun välillä muodostettua sidontaa käyttäen.

18. Patenttivaatimuksen 16 tai 17 mukainen liityntälaite, t u n n e t t u siitä, että mainittu sidonta on sidonta verkkoliitynnän MAC-osoitteen ja tunnelointi-IP-osoitteen välillä, jolloin

liityntälaite on järjestetty lähettämään tiedon mainitusta sidonnasta ARP-protokollaa tai Neighbour Discovery-protokollaa käyttäen.

(57) Tiivistelmä

Keksintö liittyy yhteysvastuun vaihtamiseen ja tunnelin päivittämiseen ensimmäisestä liityntälaitteesta toiseen liityntälaitteeseen. Ensimmäisestä liityntälaitteesta siirretään tunneliin liittyviä tunnelointiattribuutteja, ainakin vastinsolmun IP-osoite ja päätelaitteelle ensimmäisessä liityntälaitteessa allokoitu tunnelointi-IP-osoite, toiseen liityntälaitteeseen, kun on havaittu tarve vaihtaa päätelaitteen langaton yhteys toisen liityntälaitteen toteutettavaksi. Toisessa liityntälaitteessa määritetään sidonta tunnelointi-IP-osoitteen ja toisen liityntälaitteen verkkoliitynnän välille. Tietoja päätelaitteelle/päätelaitteelta vastinsolmulta/vastinsolmulle siirretään toiselle liityntälaitteelle järjestettyä sidontaa käyttäen.
(Kuvio 4)

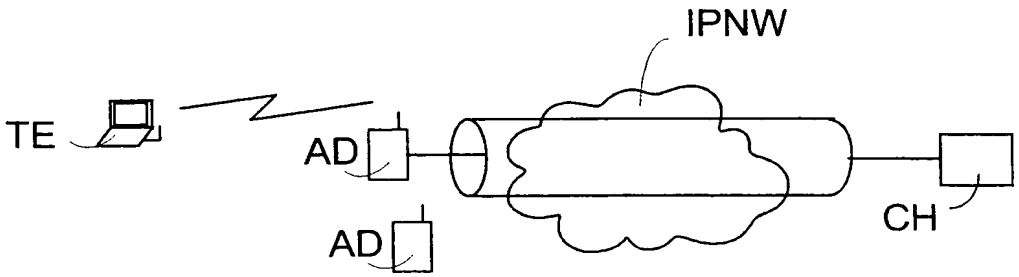
IPNW
TE
AD
AD
CH

Fig. 1

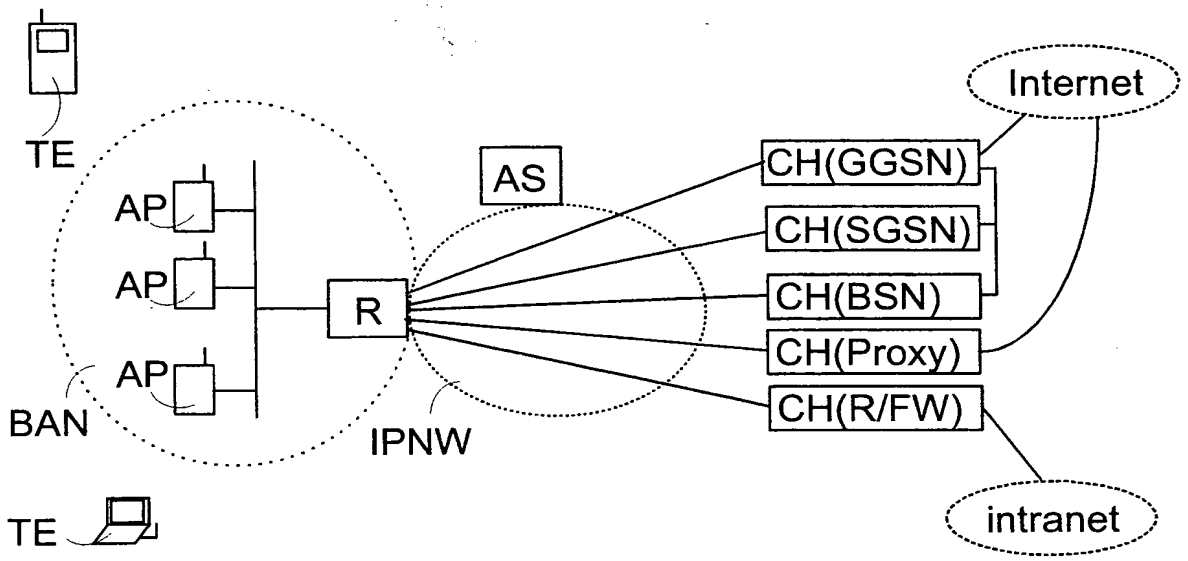
TE
AP
AP
AP
BAN
R
AS
IPNW
TE
Internet
CH(GGSN)
CH(SGSN)
CH(BSN)
CH(Proxy)
CH(R/FW)
intranet

Fig. 2

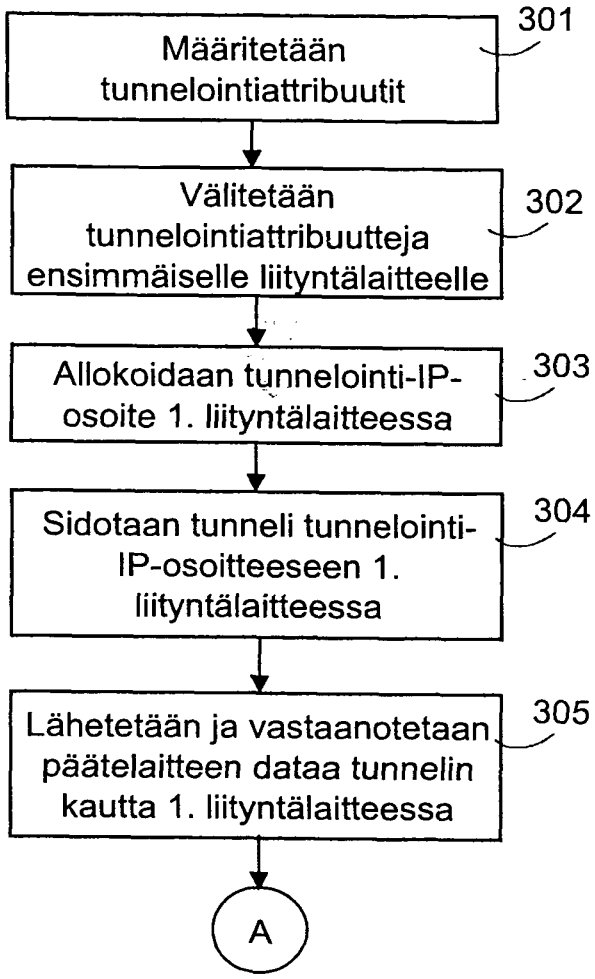
Määritetään tunnelointiattribuutit
301
Välitetään tunnelointiattribuutteja ensimmäiselle liityntälaitteelle
302
Allokoidaan tunnelointi-IP-osoite 1. liityntälaitteessa
303
Sidotaan tunneli tunnelointi-IP-osoitteeseen 1. liityntälaitteessa
304
Lähetetään ja vastaanotetaan päätelaitteen dataa tunnelin kautta 1. liityntälaitteessa
305
A

Fig. 3

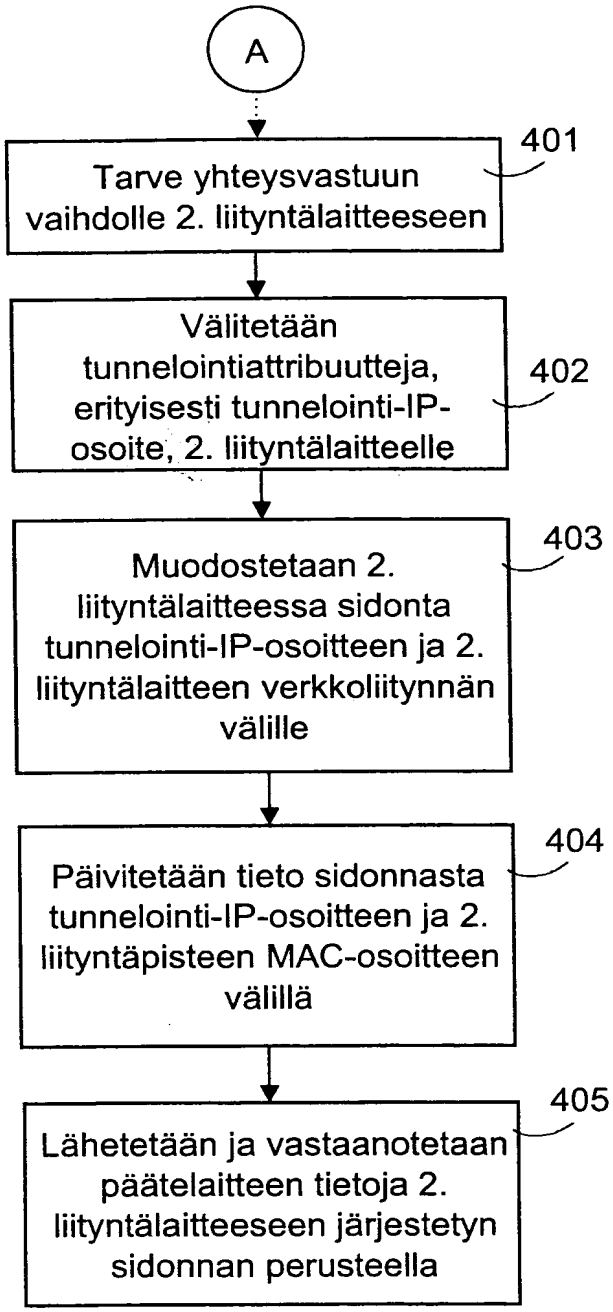
A
401
Tarve yhteysvastuun vaihdolle 2. liityntälaitteeseen
Välitetään tunnelointiattribuutteja, erityisesti tunnelointi-IP-osoite, 2. liityntälaitteelle
402
Muodostetaan 2. liityntälaitteessa sidonta tunnelointi-IP-osoitteen ja 2. liityntälaitteen verkkoliitynnän välille
403
Päivitetään tieto sidonnasta tunnelointi-IP-osoitteen ja 2. liityntäpisteen MAC-osoitteen välillä
404
Lähetetään ja vastaanotetaan päätelaitteen tietoja 2. liityntälaitteeseen järjestetyn sidonnan perusteella
405

Fig. 4

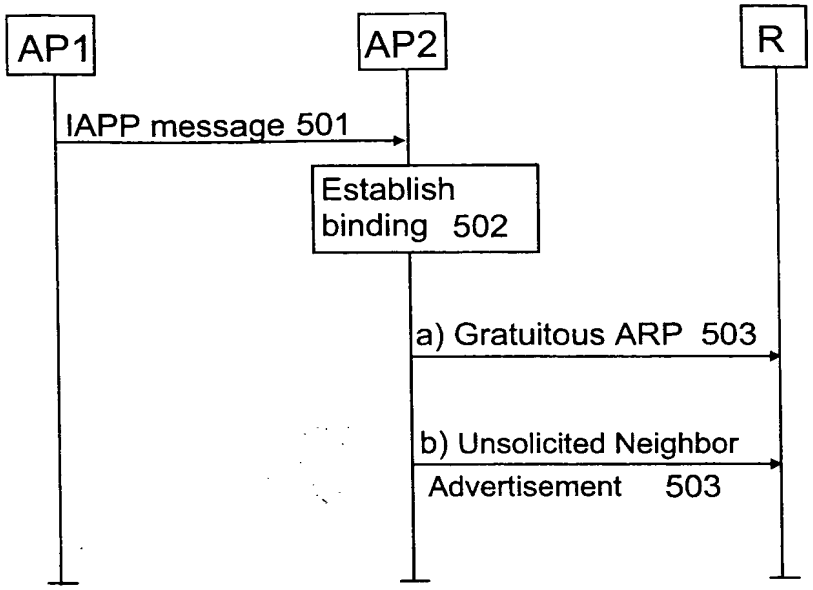
AP1
AP2
R
IAPP message 501
Establish binding 502
a) Gratuitous ARP 503
b) Unsolicited Neighbor Advertisement 503

Fig. 5